What Is Claimed Is:

1. A method of enrollment comprising:

bundling an identification (ID) request for a computer having firmware and a trusted platform module (TPM);

sending said ID request to a privacy certificate authority;

receiving a verified and signed ID from said privacy certificate authority; and

installing said verified and signed ID on said firmware.

2. The method of claim 1, wherein said verified and signed ID is installed in at least one of extensible firmware interface (EFI)-based firmware, IEEE 1275 open firmware, LinuxBios, or a PC/AT BIOS.

3. The method of claim 1, wherein bundling an ID request comprises bundling at least one of a new public ID key, an endorsement certificate, a platform certificate, or a conformance certificate into said ID request.

4. The method of claim 3, wherein said new public ID key is a public portion of an attestation identity key (AIK), said AIK having a public portion and a private portion, wherein said private portion is maintained by said TPM.

5. A method of attestation comprising:

connecting a computer having firmware and a trusted platform module (TPM) coupled to said firmware to a network;

determining a current platform trust state for said computer, wherein said current platform trust state is based on a current state of said firmware;

receiving a challenge from a challenger on said network, wherein said challenger holds an enrolled platform trust state for said computer;

signing said current platform trust state with a private portion of an attestation identity key (AIK);

providing said signed current platform trust state to said challenger; and

accessing said network when said signed current platform trust state matches said enrolled platform trust state.

6. The method of claim 5, wherein said TPM comprises a plurality of platform configure registers (PCR) and determining a current platform trust state comprises:

performing a hash-extend operation on contents of said PCRs.

7. The method of claim 5, further comprising:

provisioning said computer across said network.

8. A method of provisioning, comprising:

detecting a new computer on a network;

challenging said new computer;

receiving a current platform trust state, signed with a private portion of an attestation identity key (AIK), from said new computer;

comparing said signed current platform trust state with an enrolled platform trust state, wherein said enrolled platform trust state is signed by a privacy certificate authority; and

allowing said new computer to access said network when said enrolled platform trust state and said signed current platform trust state match.

9. The method of claim 8, further comprising:

verifying trust in said privacy certificate authority; and

allowing said new computer to access said network when said privacy certificate authority is trustworthy.

10. An apparatus, comprising:

a processor;

firmware, coupled to said processor;

a trusted platform module (TPM), coupled to said firmware;

a plurality of platform configuration registers (PCR) coupled to said TPM, wherein said PCRs contain a platform state; and

an attestation identity key (AIK), maintained by said TPM, wherein said AIK comprises a public and private key.

11. The apparatus of claim 10, wherein said firmware is at least one of extensible firmware interface (EFI)-based firmware, IEEE 1275 open firmware, LinuxBios, or a PC/AT BIOS.

12. The apparatus of claim 10, wherein said TPM is operative to calculate a platform trust state according to said platform state contained in said PCRs.

13. The apparatus of claim 12, wherein said firmware is operative to provide said public key of said AIK and said platform trust state without an operating system running on said processor.

14. A machine-accessible medium containing software code that, when read by a computer, causes the computer to perform a method comprising:

detecting a new computer on a network;

challenging said new computer;

receiving a current platform trust state signed with a private portion of an attestation identity key (AIK) from said new computer;

comparing said signed current platform trust state with an enrolled platform trust state, wherein said enrolled platform trust state is signed by a privacy certificate authority; and

allowing said new computer to access said network when said enrolled platform trust state and said signed current platform trust state match.

15. The machine-accessible medium of claim 14, wherein the software code causes the computer to perform the method further comprising:

verifying trust in said privacy certificate authority;

preventing said new computer from accessing said network when said privacy certificate authority is not trustworthy; and

allowing said new computer to access said network when said privacy certificate authority is trustworthy.

16. A machine-accessible medium containing software code that, when read by a computer, causes the computer to perform a method comprising:

determining a current platform trust state for a computer having firmware and a trusted platform module (TPM) coupled to said firmware, wherein said current platform trust state is based on a current state of said firmware and said computer is coupled to a network;

receiving a challenge from a challenger on said network, wherein said challenger holds an enrolled platform trust state for said computer;

signing said current platform trust state with a private portion of an attestation identity key (AIK);

providing said signed current platform trust state to said challenger; and

accessing said network when said signed current platform trust state matches said enrolled platform trust state.

17. The machine-accessible medium of claim 16, wherein said TPM comprises a plurality of platform configure registers (PCR) and determining a current platform trust state comprises:

performing a hash-extend operation on contents of said PCRs.

18. A machine-accessible medium containing software code that, when read by a computer, causes the computer to perform a method comprising:

bundling an ID request for a computer having firmware and a trusted platform module (TPM);

sending said ID request to a privacy certificate authority;

receiving a verified and signed ID from said privacy certificate authority; and

installing said verified and signed ID on said firmware.

19. The machine-accessible medium of claim 18, wherein said verified and signed ID is installed in at least one of extensible firmware interface (EFI)-based firmware, IEEE 1275 open firmware, LinuxBios, or a PC/AT BIOS.

20. The machine-accessible medium of claim 18, wherein bundling an ID request comprises bundling at least one of a new public ID key, an endorsement certificate, a platform certificate, or a conformance certificate into said ID request.

21. The machine-accessible medium of claim 18, wherein bundling an ID request comprises bundling a new public ID key, an endorsement certificate, a platform certificate, and a conformance certificate into said ID request.